UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,819	01/17/2002	Takuya Kobayashi	2002_0037A	5356

513 7590 11/03/2005

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/046,819	KOBAYASHI ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *33-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *33-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed August 16, 2005, have been fully considered but they are not persuasive.

2. Claims 33-58 are pending and have been examined, claims 1-32 have been cancelled.

Response to Amendment

3. The examiner withdraws the objection to the drawings.

4. The examiner withdraws the objection to the disclosure regarding the terms not defined and the minor informalities.

5. The examiner withdraws the objection to claim 13.

6. Woolsey et al. (US Patent Number 6,029,000, hereinafter Woolsey) teach code containing location data of a data component to be used for controlling the data processor and retrieving data based on the location data contained in the command data (columns 3-4, 10-12).

7. Assuming arguendo that Kolouch (US Patent Number 6,694,433) does not teach protected data region including an unprotection list, Applicant admits the different techniques of digital signatures and partially encrypting information (protected and unprotected data regions) were well known at the time the invention was made (pages 1-6, IDS document "How do I create a Signed Applet?"). Furthermore, Kolouch teaches using XML encryption to validate/authenticate documents (columns 2-6). Furthermore, devices transmitting/ receiving data from a server connected to a network with validity

determination units to determine whether data (command data and other data) is valid were conventional and well known.

Claim Rejections - 35 USC § 102

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 33-45 are rejected under 35 U.S.C. 102(a) as being anticipated by Woolsey.

Regarding claim 33, Woolsey teaches a transmitter/receiver operable to transmit/receive data to/from a server connected over a network (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67); a validity determination unit operable to determine whether the command data is valid (column 21, lines 1-67); a command data processing unit operable to retrieve, when said validity determination unit determines that the command data is valid, the data component specified by the command data, based on the location data contained in the command data (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67); and a data component processing unit operable to control said data processor based on the data component retrieved by said command data processing unit (column 13, lines 1-67, column 23, lines 1-43, column 24, lines 1-43).

Regarding claim 34, Woolsey teaches wherein said data component processing unit is operable to perform a screen display based on the data component retrieved by said command data processing unit (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 35, Woolsey teaches wherein said data component processing unit is operable to output the data component retrieved by said command data processing unit to the outside of said data processor (column 13, lines 1-67, column 23, lines 1-43, column 24, lines 1-43).

Regarding claim 36, Woolsey teaches wherein the data component used for controlling said data processor by said data component processing unit is limited to be the data component retrieved by said command data processing unit (column 13, lines 1-67, column 23, lines 1-43, column 24, lines 1-43).

Regarding claim 37, Woolsey teaches the command data is encrypted; and said validity determination unit is operable to determine whether the command data is valid after decrypting the encrypted command data (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 38, Woolsey teaches wherein said command data processing unit includes a language processing section operable to interpret a JAVA language, and a JAVA applet to be processed by said language processing section (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 39, Woolsey teaches wherein said transmitter/receiver is operable to receive, in accordance with a user's instruction, the JAVA applet included in said command data processing unit (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 40, Woolsey teaches wherein said transmitter/receiver is operable to receive, in accordance with a user's instruction, the command data to be

supplied to said validity determination unit (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 41, Woolsey teaches wherein said command data processing unit is operable to retrieve the data component from the server by using said transmitter/receiver (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 42, Woolsey teaches said command data processing unit is operable to determine whether retrieved command data is valid, and when said command data processing unit determines that the retrieved data component is valid, said data component processing unit is operable to control said data processor based on the data component (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 43, Woolsey teaches transmitting/receiving data to/from a server connected over a network (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67); determining whether the command data is valid (column 21, lines 1-67); retrieving, when the command data is determined to be valid in said determining whether the command data is valid, the data component specified by the command data, based on the location data contained in the command data (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67); and controlling the data processor based on the data component retrieved in said retrieving of the data component (column 13, lines 1-67, column 23, lines 1-43, column 24, lines 1-43).

Regarding claim 44, Woolsey teaches wherein said retrieving of the data component retrieves the data component from the server with said transmitting/receiving of the data to/from the server (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 45, Woolsey teaches wherein said retrieving of the command data determines whether the retrieved data component is valid, and, when the data component is determined to be valid in said retrieving of the data component, said controlling of the data processor controls the data processor based on the data component (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

10. Claims 48-51 are rejected under 35 U.S.C. 102(e) as being anticipated by Kolouch.

Regarding claim 48, Kolouch teaches an unprotection list generation unit operable to generate an unprotection list which lists, by type, data that is not to be subjected to tampering detection (column 3, lines 30-67, column 4, lines 1-67); a data generation unit operable to generate data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region (column 5, lines 1-67, column 6, lines 1-67); and a transmitter operable to transmit the data generated by said data generation unit; and wherein said receiving data processor comprises: a receiver operable to receive the data transmitted from said transmitting data processor (column

3, lines 30-67, column 4, lines 1-67); a protected data authentication unit operable to detect, for the data received by said receiver, whether the data in the protected data region has been tampered by using the tampering detection information in the authentication information region (column 5, lines 1-67, column 6, lines 1-67); and an unprotected data authentication unit operable to authenticate, for the data received by said receiver, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with by said protected data authentication unit (column 5, lines 1-67, column 6, lines 1-67).

Regarding claim 49, Kolouch teaches the data generated by said data generation unit is hypertext data; and the unprotection list lists, by type, a tag included in the unprotected data region (column 5, lines 1-67, column 6, lines 1-67).

Regarding claim 50, Kolouch teaches receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection (column 3, lines 30-67, column 4, lines 1-67), the protected data region including an unprotection list which lists, by type, the data included in the unprotected data region (column 3, lines 30-67, column 4, lines 1-67) detecting, for the data received in said receiving of the data, whether the data included in the protected data region has been tampered with by using the tampering detection information included in the authentication information region (column 5, lines 1-67, column 6, lines 1-67); and authenticating, for the data received in said receiving of the data, whether the data

included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with in said detecting whether the data included in the protected data region has been tampered with (column 5, lines 1-67, column 6, lines 1-67).

Regarding claim 51, Kolouch teaches in the transmitting data processor, said method comprises generating an unprotection list which lists, by type, data that is not to be subjected to tampering detection (column 3, lines 30-67, column 4, lines 1-67); generating data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region (column 5, lines 1-67, column 6, lines 1-67); and transmitting the data generated in said generating of the data to be transmitted (column 3, lines 30-67, column 4, lines 1-67) in the receiving data processor, said method comprises receiving the data transmitted from the transmitting data processor (column 3, lines 30-67, column 4, lines 1-67) detecting, for the data received in said receiving of the data, whether the data in the protected data region has been tampered with by using the tampering detection information in the authentication information region (column 5, lines 1-67, column 6, lines 1-67); and authenticating, for the data received in said receiving of the data, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been

tampered with in said detecting whether the data in the protected data region has been tampered with (column 5, lines 1-67, column 6, lines 1-67).

Claim Rejections - 35 USC § 103

11. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

12. Claims 46, 52, and 57-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Woolsey, and further in view of Gong et al. (NPL "Going Beyond the Sandbox: an overview of the new security architecture in the JAVA development kit 1.2", hereinafter "Gong").

Regarding claim 46, Woolsey teaches a receiver operable to receive data which includes an authentication information region for including the tampering detection information (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67). Woolsey does not expressly disclose protected/unprotected regions but teaches determining valid/authenticity of data received (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67). However, Gong teaches granular permissions in JAVA (pages 3-8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to call the granular security permissions afforded by Gong as protected/unprotected data region. One of ordinary skill in the art would have been motivated do so because Gong disclose fine-grained access control, an easily configurable security policy, an easily extensible access control structure, and extension of security checks to all JAVA programs and applications (Gong, pages 1-2).

Regarding claim 52, Woolsey teaches a receiver operable to receive the data with the digital signature from a server connected over a network (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67). Woolsey does not expressly disclose a signer certificate acquiring unit operable to acquire a signer certificate indicating, by type, what data is signable by a signer of the data received by said receiver but teaches determining valid/authenticity of data received using digital signatures (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67). However, Gong teaches granular permissions in JAVA and using one or more digital signatures (pages 3-8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have certificates indicating the type of data the certificate can sign. One of ordinary skill in the art would have been motivated do so because Gong disclose fine-grained access control, an easily configurable security policy, an easily extensible access control structure, and extension of security checks to all JAVA programs and applications (Gong, pages 1-2).

Regarding claim 57, the combination of Woolsey and Gong teaches the limitations as set forth under claim 52 above. Furthermore, Woolsey teaches wherein said signer certificate acquiring unit is operable to receive the signer certificate by using said receiver (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67).

Regarding claim 58, Woolsey teaches receiving the data with the digital signature from a server connected over a network (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67). Woolsey does not expressly disclose acquiring a signer certificate indicating, by type, what data is signable by a signer of the data

received in said receiving of the data but teaches determining valid/authenticity of data received using digital signatures (column 19, lines 10-67, column 20, lines 10-67, column 21, lines 1-67). However, Gong teaches granular permissions in JAVA and using one or more digital signatures (pages 3-8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have certificates indicating the type of data the certificate can sign. One of ordinary skill in the art would have been motivated do so because Gong disclose fine-grained access control, an easily configurable security policy, an easily extensible access control structure, and extension of security checks to all JAVA programs and applications (Gong, pages 1-2).

13. Claims 47 and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Woolsey and Gong, and further in view of Kolouch.

Regarding claim 47, the combination of Woolsey and Gong does not expressly disclose hypertext data using tags to include protected/unprotected data. However, Kolouch teaches the data received by said receiver is hypertext data; and the unprotection list lists, by type, a tag included in the unprotected data region (column 5, lines 1-67, column 6, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use hyper-text data including authentication/validation information with the system of Woolsey and Gong. One of ordinary skill in the art would have been motivated do so because it was well known in the art to protect data by using tags that list the protected information (Kolouch, column 1, lines 1-67, column 2, lines 1-67).

Regarding claim 53, the combination of Woolsey and Gong does not expressly disclose wherein the signer certificate can include, in a list, by type, a plurality of the signable data. However, Kolouch teaches wherein the signer certificate can include, in a list, by type, a plurality of the signable data (column 5, lines 1-67, column 6, lines 1-67). The motivation for combining is the same as that for claim 47 above.

Regarding claim 54, the combination of Woolsey and Gong does not expressly disclose the signer certificate can include a wildcard as a type of the signable data, and when the signer certificate acquired by said signer certificate acquiring unit includes the wildcard as the type of the signable data, said signature authentication unit is operable to determine that the signature applied to any data received in said receiver is valid. However, Kolouch teaches the signer certificate can include a wildcard as a type of the signable data, and when the signer certificate acquired by said signer certificate acquiring unit includes the wildcard as the type of the signable data, said signature authentication unit is operable to determine that the signature applied to any data received in said receiver is valid (column 3, lines 30-67, column 4, lines 1-67, column 5, lines 1-67, column 6, lines 1-67). The motivation for combining is the same as that for claim 47 above.

Regarding claim 55, the combination of Woolsey and Gong does not expressly disclose wherein said signature authentication unit is operable to acquire a type of the data based on a characteristic part of a Uniform Resource Identifier of the data received by said receiver. However, Kolouch teaches wherein said signature authentication unit is operable to acquire a type of the data based on a characteristic part of a Uniform

Resource Identifier of the data received by said receiver (column 3, lines 30-67, column 4, lines 1-67, column 5, lines 1-67, column 6, lines 1-67). The motivation for combining is the same as that for claim 47 above.

Regarding claim 56, the combination of Woolsey and Gong does not expressly disclose wherein said signature authentication unit is operable to acquire the type of the data based on a header part of the data received by said receiver. However, Kolouch teaches wherein said signature authentication unit is operable to acquire the type of the data based on a header part of the data received by said receiver (column 3, lines 30-67, column 4, lines 1-67, column 5, lines 1-67, column 6, lines 1-67). The motivation for combining is the same as that for claim 47 above.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Cofta (US Patent Application Publication 2001/0016042) discloses loading program modules in a terminal using digital signatures and encryption. Shear (US Patent 6,157,721) discloses a verifying authority digitally signs a load module or other executable with several different digital signatures and/or signature schemes, a protected processing environment or other secure execution space may require a load module or other executable to present multiple digital signatures before accepting it. An attacker would have to "break" each (all) of the several digital signatures and/or signature schemes to create an unauthorized load module or other executable that would be accepted by the protected processing environment or other secure execution space. Different protected processing environments (secure execution spaces) might examine different subsets of the multiple digital signatures--so that compromising one protected processing environment (secure execution space) will not compromise all of them. As an optimization, a protected processing environment or other secure execution space might verify only one of the several digital signatures (for example, chosen at random each time an executable is used)--thereby speeding up the digital signature verification while still maintaining a high degree of security (column 6,

lines 1-67, column 7, lines 1-67). Atkinson (US Patent Number 5,892,904) discloses a certification or signing method that ensures the authenticity and integrity of a computer program.

16. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

18. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

19. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

Primary Examiner
AU2131
10/31/05